UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/005,066	12/03/2001	Julie Anna Symons	10015520	9441

22879 7590 11/05/2010

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
TRAN, NGHI V	

ART UNIT	PAPER NUMBER
2451	

NOTIFICATION DATE	DELIVERY MODE
11/05/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte JULIE ANNA SYMONS and SHARAD SINGHAL

Appeal 2009-006269[1]
Application 10/005,066
Technology Center 2400

Before JOHN A. JEFFERY, JAMES D. THOMAS, and
JOSEPH L. DIXON, *Administrative Patent Judges*.

JEFFERY, *Administrative Patent Judge*.

DECISION ON APPEAL[2]

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 13-22 and 24-38. We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

---

[1] This appeal is related to another appeal filed in connection with Application Serial Number 09/971,857 (Appeal 2009-007531). App. Br. 2, 27 (Rel. Proc. App'x). The issues in that appeal, however, are not germane to the issues before us in this appeal.

[2] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

STATEMENT OF THE CASE

Appellants' invention detects and prevents intrusion in a virtually-wired switching fabric by (1) determining unexpected packet addresses, and (2) tracing a network topology to determine the port where those packets entered the network. *See generally* Abstract; Spec. 1. Claim 13 is illustrative:

> 13. A computer-readable medium having stored thereon a program, which when run on a processor, performs a method of managing a network, said method comprising:
>
> comparing addresses associated with packets received at a first port in said network with expected addresses for said first port to determine unexpected addresses; and
>
> tracing a topology of said network to determine a second port at which a packet associated with an unexpected address entered said network.

The Examiner relies on the following as evidence of unpatentability:

Holloway	US 5,805,801	Sept. 8, 1998
Vairavan	US 2002/0083344 A1	June 27, 2002 (filed June 27, 2001)
Wang	US 6,538,997 B1	Mar. 25, 2003 (filed June 24, 1998)

THE REJECTIONS

1. The Examiner rejected claims 13-16, 18-22, and 25-30 under 35 U.S.C. § 103(a) as unpatentable over Vairavan and Wang. Ans. 3-7.[3]

[3] Throughout this opinion, we refer to (1) the Appeal Brief filed July 12, 2007; (2) the Examiner's Answer mailed March 21, 2008; and (3) the Reply Brief filed May 21, 2008.

2. The Examiner rejected claims 17, 24, and 31-38 under 35 U.S.C. § 103(a) as unpatentable over Vairavan, Wang, and Holloway. Ans. 7-12.[4]

THE OBVIOUSNESS REJECTION OVER VAIRAVAN AND WANG

Regarding representative claim 13, the Examiner finds that Vairavan discloses every recited feature except tracing a network topology to find a port at which a packet associated with an unexpected address entered the network. Ans. 3-5, 12-15. The Examiner, however, cites Wang for this feature in concluding the claim would have been obvious. *Id.*

Although Appellants acknowledge Vairavan's various packet filtering capabilities, Appellants maintain that these filtering techniques do not compare packet addresses with expected addresses for a first port to determine unexpected addresses as claimed. App. Br. 10-12; Reply Br. 1. Appellants also argue that the cited prior art does not trace a network topology to determine a second port at which a packet associated with an unexpected address entered the network as claimed. App. Br. 12-14. In this regard, Appellants emphasize that Wang's tracing functionality is merely for troubleshooting or diagnostic purposes, and does not teach or suggest the recited topology tracing limitation. *Id.* The issues before us, then, are as follows:

[4] Although the Examiner presents two separate rejections based on these references (*compare* Ans. 7 *with* Ans. 8), we nonetheless consolidate these rejections here for clarity and brevity.

ISSUES

Under § 103, has the Examiner erred in rejecting claim 13 by finding that Vairavan and Wang collectively would have taught or suggested:

(1) comparing received packet addresses with expected addresses for a first port to determine unexpected addresses, and

(2) tracing a network topology to determine a second port at which a packet associated with an unexpected address entered the network?

FINDINGS OF FACT (FF)

1. Vairavan's inter/intra networking device 110 couples various types of networks (e.g., copper-based, optical, and wireless) into a single enterprise infrastructure. Vairavan, ¶¶ 0003, 0046-47; Fig. 1.

2. Networking device 110 includes packet processor 210 coupled to security interface 225 that is, in turn, coupled to security processor 235. The packet processor performs various packet analyses and functions upon receiving packets including analyzing their destination addresses to route the packets. Vairavan, ¶¶ 0054-58; Fig. 2.

3. Packet processor 210 includes security policy database 315 comprising standards for specifying packet-filtering rules based on information found within a packet header (e.g., source and destination addresses). Security standards may include (1) discarding all source-routed packets; (2) discarding all incoming packets from a local network; (3) passing all packets that are part of an existing TCP connection, etc. Vairavan, ¶¶ 0074-79; Fig. 3.

4. Security policy database 315 may also contain an IPsec processing table whose entries include a set of parameters that support security association management using a destination IP address (which may be a range of addresses as well as a wildcard address), a source IP address, etc. Vairavan, ¶¶ 0080-84; Fig. 3.

5. The packet processor's firewall module 310 analyzes, isolates, and discards packets according to security standards and filtering techniques within different firewall layers. In addition to providing a network address translation (NAT) function to map incoming IP addresses to local VPN addresses, the firewall module can also identify, authenticate, and control access of received packets. Vairavan, ¶ 0086; Fig. 3.

6. Firewall module 310 uses various filtering algorithms including (1) packet content filtering, (2) stateful packet inspection; and (3) network intrusion detection. Vairavan, ¶¶ 0088-90; Fig. 3.

7. The content filtering algorithm filters packets according to information within the packet header (e.g., specific IP addresses). As such, a user may be denied access to a particular site before leaving the firewall by comparing IP addresses to a table defining access rights. Vairavan, ¶ 0088.

8. The stateful inspection filtering algorithm identifies states that the packet has completed. To this end, the packet's various states or histories are monitored to identify an attack pattern used to hack into various devices on an attached network. IP spoofing detection monitors packets sent from a particular source to various devices within a network. Vairavan, ¶ 0089.

9. Network intrusion detection monitors packets transmitted to or from specific devices on the enterprise, and is based on (1) anomaly detection, and (2) misuse detection. Misuse detection identifies predefined

known attack patterns in packet traffic (e.g., by monitoring for large numbers of TCP connection requests to many different ports on a particular device, thereby identifying someone attempting a TCP port scan). Vairavan, ¶ 0090.

10. Traces are used to help troubleshoot problems in computer networks. To this end, an "mtrace" can be used that starts at a path's destination and received at the other end. Wang, col. 1, ll. 10-27.

11. A layer-2 trace can be used by hosts and/or switches and/or routers to gather (1) general information related to a switched network, or (2) specific diagnostic information relating to the particular path through the switched network. Wang, col. 6, ll. 17-21.

12. Wang notes that, in connection with layer-2 multicast traces, bridges/switches know over which port a particular (unicast) medium access control (MAC) address is reachable. If they do not, the frame is "flooded" over all outgoing non-blocked ports. Wang, col. 1, ll. 46-48; col. 6, ll. 59-63.

13. If a multicast trace is requested between two points on a multicast tree, the trace request is forwarded over (1) a specific port leading to the specified destination, or (2) all outgoing ports of the distribution tree. Wang, col. 8, ll. 39-44; Figs. 5a-5b.

14. Response data for a layer-2 trace includes (1) the incoming port (the port over which the trace request arrived), and (2) the outgoing port (the port over which the trace request is forwarded). Wang, col. 9, ll. 38-47; Fig. 6b.

ANALYSIS

Based on the record before us, we find no error in the Examiner's obviousness rejection of representative claim 13. First, we agree with the Examiner that the functionality of Vairavan's packet processor firewall module reasonably suggests comparing received packet addresses with *expected* addresses for a first port to determine *unexpected* addresses as claimed.

We note at the outset that Appellants have pointed to no definition of the term "expected" in the Specification. Nor have Appellants disputed the Examiner's cited definition of the term "unexpected" which means "not to anticipate or look forward to the coming or occurrence of." Ans. 13. We therefore adopt the Examiner's plain-meaning construction of the term "unexpected."

As the Examiner indicates (Ans. 12), Vairavan's firewall module analyzes, isolates, and discards packets according to security standards and filtering techniques within different firewall layers. FF 5. To this end, the firewall module uses various filtering techniques and algorithms (FF 3, 6) that filter packets according to (1) particular IP addresses within the packet's header (FF 3, 4, 7); (2) particular states or histories of packets (FF 8); and (3) packets transmitted to, or received from, specific devices (e.g., ports on a particular device) (FF 9).

As the Examiner indicates (Ans. 12), performing the requisite comparisons and actions associated with these address-based filtering techniques would involve determining whether the compared addresses were "expected" or not—at least with respect to the standard to which the comparison was made.

That is, identifying particular addresses as a basis to filter packets by comparing associated addresses would, in effect, compare those addresses with a known standard (i.e., "expected" addresses) to determine "unexpected" addresses, namely those addresses which do not comport with that standard. *See* FF 3-9. And it is packets from those "unexpected" addresses that Vairavan's system deems problematic and therefore filters. *See id.* Notably, Vairavan also identifies these problematic packets with respect to their unauthorized introduction via different ports on particular devices (e.g., a hacker attempting a TCP port scan). *See* FF 9.

Although this port-based functionality in Vairavan at least suggests tracing the topology to determine the port(s) where these "unexpected" packets entered the network, we nonetheless are not persuaded of error in the Examiner's reliance on Wang for this feature. While Wang indicates that traces are used for troubleshooting and diagnostic purposes (FF 10-11), we nevertheless see no reason why such tracing techniques could not be used to determine ports where "unexpected" packets entered Vairavan's network, particularly since Wang's tracing techniques identify relevant ports (FF 12-14). We reach this conclusion noting Vairavan's filtering and misuse detection schemes are based on monitoring packet traffic involving particular paths and devices. *See* FF 3-9. Enhancing this monitoring via tracing techniques such as those disclosed by Wang is tantamount to the predictable use of prior art elements according to their established functions—an obvious improvement. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

We are therefore not persuaded that the Examiner erred in rejecting representative claim 13, and claims 14-16, 18-22, and 25-30 not separately argued.

THE OBVIOUSNESS REJECTION OVER VAIRAVAN, WANG, AND HOLLOWAY

We will also sustain the Examiner's rejection of claims 17, 24, and 31-38 over Vairavan, Wang, and Holloway (Ans. 7-12). Although Appellants argue that Holloway does not cure the previously-alleged deficiencies of Vairavan and Wang (App. Br. 14-19), we are unpersuaded by these arguments for the reasons noted previously. For similar reasons, we are also unpersuaded of error in the Examiner's position regarding the commensurate limitations of claim 31 as well as the recited management agent functionality. Ans. 8-10, 14-17.

We are therefore not persuaded that the Examiner erred in rejecting 17, 24, and 31-38.

CONCLUSION

The Examiner did not err in rejecting claims 13-22 and 24-38 under § 103.

ORDER

The Examiner's decision rejecting claims 13-22 and 24-38 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

pgc

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528